U.S. Department of Justice

Criminal Division

Child Exploitation and Obscenity Section

1400 New York Ave., NW
Suite 600
Washington, DC 20530
(202) 514-5780 FAX: (202) 514-1793

November 7, 2014

Dear Counsel:

Pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure, the government hereby discloses that it intends to elicit testimony from Federal Bureau of Investigation ("FBI") Special Agent ("SA") Steven A. Smith, Jr. and FBI Supervisory Special Agent ("SSA") P. Michael Gordon, under Federal Rules of Evidence 702, 703, or 705. Pursuant to Rule 16(b)(1)(C) of the Federal Rules of Criminal Procedure, the government hereby requests from defendant disclosure of testimony he intends to use under Rule 702, 703 and/or 705 of the Federal Rules of Evidence as evidence at trial.

The CVs of SA Smith and SSA Gordon are attached. Their testimony will be based upon their respective knowledge, skills, training and experience in the areas of computer forensics, computer programming, computer networking and network management and analysis, computer forensic data acquisition and analysis, investigations in child exploitation cases, the Internet, and forensic analysis of digital media including computers, computer servers, and websites. They may also testify regarding the Internet, the forensic examination of computers and digital media, and how the Internet is used to trade child pornography. Specifically, they may testify about the following topics:

- The Onion Router ("Tor") anonymity network, including its origin, structure, function, configuration and software applications; the Tor browser bundle; other methods to access the Tor network, such as tor2web and onion.to; and investigative strategies to identify users of the Tor network. Please note that detailed information about the Tor network, its structure and function, is publicly available at the Tor project website, www.torproject.org.

- the structure, operation, monitoring and seizure of data from the websites your clients are charged with accessing. Such testimony may include a description of the structure, function, and content of the website, including the child pornography available (as further described in your client's Indictment, the search warrant affidavit authorizing the deployment of a Network Investigative Technique on the pertinent website, and the search warrant affidavit authorizing a search of your client's residence, all of which you have been provided through discovery); unique session identifiers that track a user's activity on the site; the particular web pages accessed by a user during one of those sessions; and particular child pornography images/videos accessed by a user during one of those sessions. Such testimony may include but not be limited to the operation of websites, computers and computer servers, and related technical terms/concepts including HTML, HTTP,

PHP, Flash, and Javascript. Please note that a working offline copy of each of those websites has been made available to you and/or an expert of your choosing for examination. Further, through discovery, you were provided reports documenting data obtained from those computer servers, including data pertinent to your client's actions on the site. In addition, as we have previously advised you, the computer server(s) that hosted the websites are, and remain, available for examination by you or your chosen expert.

- the "Network Investigative Technique" ("NIT") that was deployed on each website and the admission of evidence obtained through the use of that technology. Such testimony may include: technical concepts underlying the use of technology such as the NIT, including but not limited to Flash, TCP, proxy servers, IP addresses, web browsers, computer servers, and exploits; the programming and operation of websites and computer servers; and the programming, testing and deployment of computer code on websites and computer servers; the configuration and deployment of the particular NIT utilized on the websites your clients accessed; and pre-deployment testing performed regarding the particular NIT utilized on the websites your clients accessed.

You have previously been provided reports documenting data obtained via the use of the NIT, which includes IP address information, session identifier information, operating system and architecture type. We have also previously disclosed to you via e-mails dated September 4, 2014, and September 23, 2014, incorporated herein by reference, details regarding where the particular NIT code was obtained and how it operated. In particular, as described in my September 4, 2014, e-mail message, the technique utilized a Flash application that, when downloaded by a user and activated by their browser, made a direct TCP connection to a server that the FBI controlled. Depending on the operating system and version of the user's browser, the connection would bypass the browser's configured proxy server and reveal the user's true IP address. In addition, the NIT also sent the user's operating system name and architecture type. Please also see my September 4, 2014 e-mail for example programming code for the Flash application itself. Further, as noted above and in my September 4 and 23 e-mails, the computer servers that hosted the pertinent websites contain the compiled code for the NIT. Those servers have been, and remain, available for examination by an expert of your choice. The experts disclosed herein may testify based upon their knowledge, skills, training and experience, as to any matters disclosed therein.

In order to avoid any confusion regarding the operation of the NIT, I offer the following further description of its functionality, about which the experts disclosed herein may testify.

The NIT was a Flash application. Flash applications are commonly present on numerous Internet websites. The NIT did not consist of a virus or "malware."

The NIT took advantage of a potential vulnerability in the configuration of a user's computer. When a user accessed a page on one of the pertinent websites where the NIT had been deployed, the NIT computer code would be downloaded to a user's computer along with the images/text/content that made up that web page. If a user's web browser was not configured to block Flash applications, then the NIT, once downloaded by a user's computer, would cause the computer to send a communication (in other words, a request) to a government-controlled computer that revealed the computer's IP address, a session identifier, the computer's operating

system and architecture. If a user's web browser was configured to block Flash applications, then the NIT would not successfully cause the computer to send such a request. As of November of 2012, the up-to-date Tor browser bundle was configured to block such Flash applications. Accordingly, the NIT would not have revealed the IP address of such a user, or of a user who had manually configured his/her browser to connect to the Tor network and opted to block Flash applications. Because none of your clients were using the up-to-date Tor browser bundle to access the website in question, and none of your clients configured his computer to block Flash applications, the NIT successfully identified your client's IP address.

Special Agent Smith and Supervisory Special Agent Gordon may also testify based upon their knowledge, skills, training and experience in the area of computer forensics, computer forensic data acquisition and analysis, investigations in child exploitation cases, and the Internet, as to the following matters:

- regarding the Internet, which is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information;

- that connections between Internet computers exist across state and international borders; and that the Internet is a means of interstate and international communication; indeed, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state;

- regarding modems, and how a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world;

- regarding Internet Service Providers. Individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format;

- regarding IP Addresses. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses;

- that when a customer logs into the Internet using the service of an ISP, the computer used

by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period;

- regarding four basic functions computers and the Internet serve in connection with child pornography: production, communication, distribution, and storage;

- regarding how individuals can use computers and the Internet to meet, communicate with each other, and share files, including but not limited to websites, chat rooms, message boards, email, instant messaging, news groups, social networking sites, peer-to-peer programs, ICQ;

- regarding how child pornographers can transfer non-digital photographs from a camera into a computer-readable format a scanner, and how digital cameras allow images to be transferred directly onto a computer. Digital cameras often embed information into digital pictures, known as metadata, that identifies the camera used to take the picture;

- regarding how a computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images and videos at very high resolution;

- regarding how digital images/videos can be stored on external storage media such as thumb drives, compact disks, external hard drives, mp-3 players, smart phones, and how digital images/videos can be easily transferred from one digital device to another;

- regarding dedicated online storage space, such as the "FTP," or "File Transfer Protocol" site, and how such a site allows Internet users to maintain a massive and secure private library of child pornography that is available for viewing or download only by a certain group of individuals, such as members of the PedoBook online bulletin board;

- regarding user-created message boards, and how they can be easily created with free or inexpensive software and commercial web hosting companies;

- regarding forensic hashing, which is the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data (such as a particular file). If the data is changed, even very slightly (such as the addition or deletion of a comma or a period), the identifier should change. A hash value can be thought of as a "digital fingerprint" for data;

- regarding the use of a "hash set" which contains the hash values of image and video files associated with known identified victims of child pornography to determine whether these files are stored within a digital device;

- The process of obtaining and verifying an image of a computer media item, bit-stream copies, and Message-Digest algorithm 5 (MD5) hash values;

- Specialized computer terms, including, but not limited to, terms mentioned in this notice and in his report, such as ".html," ".lnk" ".jpg," ".mpg," ".avi," "cookie file," and "file slack;"

- Evidence of web browsing activity and e-mail communications, including, but not limited to, fragments of web pages accessed, cookie files, e-mail messages, and other Internet-based communications stored in locations including, but not limited to, the temporary Internet file folders, file slack, and unallocated space;

- The operation, analysis and investigation of websites, bulletin boards, social networking platforms and other Internet technologies dedicated to the sexual exploitation of children;

- Online undercover tactics and techniques pertinent to the investigation, identification and apprehension of suspects engaging in online sexual exploitation of children;

- Methods, tactics and techniques of individuals who seek to exploit children online.

Please contact me, Assistant U.S. Attorney Michael Norris or Trial Attorney Sarah Chang or if you have any questions about any of the information provided.

Sincerely,

/s/ Keith Becker
Keith Becker
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division
United States Department of Justice

Enclosures